1 1. (Currently Amended) A method of comparing access control lists to configure a
2   security policy on a network, the method comprising the computer-implemented steps
3   of:
4   identifying first sub-entries in a first access control list;
5   identifying second sub-entries in a second access control list;
6   programmatically determining whether a first access control list is functionally
7   equivalent to a second access control list in order to configure the security
8   policy on the network by determining whether each first sub-entry in the first
9   access control list is equivalent to at least one of the second sub-entries; and
10   determining that the first access control list is functionally equivalent to the second
11   access control list only when each of the first sub-entries is equivalent to at
12   least one of the second sub-entries;
13   wherein programmatically determining whether the first access control list is
14   equivalent to the second access control list comprises:
15   identifying a dimensional range for each policy action specified in the first
16   access control list, the dimensional range of each policy action
17   characterizing communication packets specified by entries in the first
18   access control list for that policy action;
19   identifying a dimensional range for each policy action specified in the second
20   access control list, the dimensional range of each policy action
21   characterizing communication packets specified by entries in the
22   second access control list for that policy action; and
23   determining whether the dimensional range identified for each policy action in
24   the first access control list is equivalent to the dimensional range
25   identified for each policy action in the second access control list;
26   wherein identifying the dimensional range for each policy action specified in the first
27   access control list and in the second access control list comprises at least one
28   step from a set of steps comprising:

29	identifying a source Internet Protocol (IP) address range and a destination IP
30	address range for communication packets specified by each of the
31	entries in the first access control list and in the second access control
32	list;
33	identifying a source port range and a destination port range for
34	communication packets specified by each of the entries in the first
35	access control list and in the second access control list; and
36	identifying a communication protocol for communication packets specified by
37	each of the entries in the first access control list and in the second
38	access control list.

| 1 | 2-5. | (Canceled) |

1	6.	(Previously Presented) A method as recited in Claim 1, wherein the first access
2		control list and the second access control list each specify a plurality of entries, and
3		each entry identifies a dimensional range for a policy action, the dimensional range
4		characterizing communication packets that are to be affected by the policy action, and
5		wherein programmatically determining whether a first access control list is equivalent
6		to the second access control list includes:
7		determining whether each entry in the first access control list has a dimensional range
8		that is either equivalent to or contained by the dimensional range of entries in
9		the second access control list that specify the policy action of the entry in the
10		first access control list.

1	7.	(Previously Presented) A method as recited in Claim 1, wherein the first access
2		control list and the second access control list each specify a plurality of entries, and
3		each entry identifies a dimensional range for a policy action, the dimensional range
4		characterizing communication packets that are to be affected by the policy action, and
5		wherein programmatically determining whether a first access control list is equivalent
6		to the second access control list includes:
7		determining whether each entry in the first access control list has a dimensional range
8		that is either equivalent to or contained by the dimensional range of entries in

9   the second access control list that specify the policy action of the entry in the

10   first access control list; and

11   determining whether each entry in the second access control list has a dimensional

12   range that is either equivalent to or contained by the dimensional range of

13   entries in the first access control list that specify the same policy action.

1   8.   (Canceled)

1   9.   (Currently Amended) A~~n apparatus for~~ method of comparing access control lists to

2   configure a security policy on a network, the apparatus ~~method~~ comprising:

3   a processor;

4   a network interface that communicatively couples the processor to the network to

5   receive flows of packets therefrom;

6   a memory; and

7   sequences of instructions in the memory which, when executed by the processor,

8   cause the processor to carry out steps of:

9   identifying a dimensional range and a policy action for each entry in a first

10   access control list;

11   identifying all overlapping dimensional ranges in the first access control list,

12   each overlapping dimensional range corresponding to where the

13   dimensional ranges of entries in the first access control list overlap;

14   identifying all non-overlapping dimensional ranges in the first access control

15   list, each of the non-overlapping dimensional ranges corresponding to

16   dimensional ranges of entries in the first access control list that do not

17   overlap dimensional ranges of other entries in the first access control

18   list;

19   identifying a policy action for each identified overlapping dimensional range

20   of the first access control list;

21   identifying a policy action for each identified non-overlapping dimensional

22   range of the first access control list; and

23   determining whether each identified overlapping and non-overlapping

24   dimensional range identified from the first access control list is

25	contained by or equal to a dimensional range of entries in a second
26	access control list in which the entries of the second access control list
27	have the policy action of that identified overlapping or non-
28	overlapping dimensional range;
29	wherein identifying a policy action for each identified overlapping dimensional range
30	of the first access control list includes using a conflict rule to determine the
31	policy action from a first policy action of a first entry having a dimensional
32	range within the overlapping dimensional range, and from a second policy
33	action of a second entry having a dimensional range within the overlapping
34	dimensional range, wherein the second policy conflicts with the first policy;
35	wherein using the conflict rule to determine the policy action comprises selecting one
36	of the first policy and the second policy based on a selected policy of the first
37	and second policies being newer than an unselected policy of the first and
38	second policies.

1	10.	(Currently Amended) An apparatus method as recited in Claim 9, wherein the steps
2		further comprising comprise:
3		identifying a dimensional range and a policy action for each entry in the second
4		access control list;
5		identifying all overlapping dimensional ranges in the second access control list, each
6		overlapping dimensional range corresponding to where the dimensional
7		ranges of entries in the second access control list overlap;
8		identifying all non-overlapping dimensional ranges in the second access control list,
9		each of the non-overlapping dimensional ranges corresponding to dimensional
10		ranges of entries in the second access control list that do not overlap
11		dimensional ranges of other entries in the second access control list;
12		identifying a policy action for each identified overlapping dimensional range in the
13		second access control list;
14		identifying a policy action for each identified non-overlapping dimensional range of
15		the second access control list; and
16		determining whether each identified overlapping and non-overlapping dimensional
17		range identified from the second access control list is contained by or equal to

18		a dimensional range of entries in the first access control list in which the
19		entries of the first access control list have the policy action of that identified
20		overlapping or non-overlapping dimensional range.

1   11.   (Currently Amended) A~~ apparatus~~ method~~ as recited in Claim 9, wherein the steps

2   further comprise:

3   identifying a dimensional range and a policy action for each entry in the second

4   access control list;

5   identifying all overlapping dimensional ranges in the second access control list, each

6   overlapping dimensional range corresponding to where the dimensional

7   ranges of entries in the second access control list overlap;

8   identifying all non-overlapping dimensional ranges in the second access control list,

9   each of the non-overlapping dimensional ranges corresponding to dimensional

10   ranges of entries in the second access control list that do not overlap

11   dimensional ranges of other entries in the second access control list;

12   identifying a policy action for each identified overlapping dimensional range of the

13   second access control list;

14   identifying a policy action for each identified non-overlapping dimensional range of

15   the second access control list; and

16   wherein determining whether each identified overlapping and non-overlapping

17   dimensional range of the first access control list is contained by or equal to a

18   dimensional range of entries in a second access control list includes

19   determining whether each identified overlapping and non-overlapping

20   dimensional range identified from the first access control list is contained by

21   or equal to overlapping and non-overlapping dimensional ranges of the second

22   access control list.

1   12-13. (Canceled)

1   14.   (Currently Amended) A~~ apparatus~~ method~~ as recited in Claim 9, wherein

2   identifying a dimensional range and a policy action for each entry in the first access

3   control list includes identifying a source address range and a destination address

4 range for communication packets specified by each of the entries in the first access

5 control list.

1 15. (Currently Amended) A<u>n apparatus</u> ~~method~~ as recited in Claim 9, wherein

2 identifying a dimensional range and a policy action for each entry in the first access

3 control list includes identifying a source port range and a destination port range for

4 communication packets specified by each of the entries in the first access control list.

1 16. (Currently Amended) A<u>n apparatus</u> ~~method~~ as recited in Claim 9, wherein

2 identifying a dimensional range and a policy action for each entry in the first access

3 control list includes identifying a communication protocol for communication packets

4 specified by each of the entries in the first access control list.

1 17. (Currently Amended) A computer readable medium for comparing access control

2 lists to configure a security policy on a network, the computer readable medium

3 carrying instructions for performing the steps of:

4 identifying first sub-entries in a first access control list;

5 identifying second sub-entries in a second access control list;

6 programmatically determining whether a first access control list is functionally

7   equivalent to a second access control list in order to configure the security

8   policy on the network by determining whether each first sub-entry is

9   equivalent to at least one of the second sub-entries; and

10 determining that the first access control list is functionally equivalent to the second

11   access control list only when each of the first sub-entries is equivalent to at

12   least one of the second sub-entries<u>;</u>

13 <u>wherein programmatically determining whether the first access control list is</u>

14   <u>equivalent to the second access control list comprises:</u>

15   <u>identifying a dimensional range for each policy action specified in the first</u>

16   <u>access control list, the dimensional range of each policy action</u>

17   <u>characterizing communication packets specified by entries in the first</u>

18   <u>access control list for that policy action;</u>

19   <u>identifying a dimensional range for each policy action specified in the second</u>

20   <u>access control list, the dimensional range of each policy action</u>

21	characterizing communication packets specified by entries in the
22	second access control list for that policy action; and
23	determining whether the dimensional range identified for each policy action in
24	the first access control list is equivalent to the dimensional range
25	identified for each policy action in the second access control list;
26	wherein identifying the dimensional range for each policy action specified in the first
27	access control list and in the second access control list comprises at least one
28	step from a set of steps comprising:
29	identifying a source Internet Protocol (IP) address range and a destination IP
30	address range for communication packets specified by each of the
31	entries in the first access control list and in the second access control
32	list;
33	identifying a source port range and a destination port range for
34	communication packets specified by each of the entries in the first
35	access control list and in the second access control list; and
36	identifying a communication protocol for communication packets specified by
37	each of the entries in the first access control list and in the second
38	access control list.

1	18-24.	(Canceled)

1	25.	(Currently Amended) A computer system for comparing access control lists to
2		configure a security policy on a network, the computer system comprising:
3		means for identifying first sub-entries in a first access control list;
4		means for identifying second sub-entries in a second access control list;
5		means for programmatically determining whether a first access control list is
6		functionally equivalent to a second access control list in order to configure the
7		security policy on the network by determining whether each first sub-entry is
8		equivalent to at least one of the second sub-entries; and
9		means for determining that the first access control list is functionally equivalent to the
10		second access control list only when each of the first sub-entries is
11		equivalent to at least one of the second sub-entries;

12   wherein the means for programmatically determining whether the first access control

13   list is equivalent to the second access control list comprise:

14   means for identifying a dimensional range for each policy action specified in

15   the first access control list, the dimensional range of each policy action

16   characterizing communication packets specified by entries in the first

17   access control list for that policy action;

18   means for identifying a dimensional range for each policy action specified in

19   the second access control list, the dimensional range of each policy

20   action characterizing communication packets specified by entries in

21   the second access control list for that policy action; and

22   means for determining whether the dimensional range identified for each

23   policy action in the first access control list is equivalent to the

24   dimensional range identified for each policy action in the second

25   access control list;

26   wherein the means for identifying the dimensional range for each policy action

27   specified in the first access control list and the means for identifying the

28   dimensional range for each policy action specified in the second access

29   control list comprises at least one means from a set of means comprising:

30   means for identifying a source Internet Protocol (IP) address range and a

31   destination IP address range for communication packets specified by

32   each of the entries in the first access control list and in the second

33   access control list;

34   means for identifying a source port range and a destination port range for

35   communication packets specified by each of the entries in the first

36   access control list and in the second access control list; and

37   means for identifying a communication protocol for communication packets

38   specified by each of the entries in the first access control list and in the

39   second access control list.

1   26.   (Currently Amended) A policy server communicatively coupled to security devices

2   in a network to configure a security policy on a network, the policy server

3   comprising:

4	a processor;
5	a network interface that communicatively couples the processor to the network to
6	receive flows of packets therefrom;
7	a memory; and
8	sequences of instructions in the memory which, when executed by the processor,
9	cause the processor to carry out the steps of:
10	identifying first sub-entries in a first access control list;
11	identifying second sub-entries in a second access control list;
12	programmatically determining whether a first access control list is
13	functionally equivalent to a second access control list in order to
14	configure the security policy on the network by determining whether
15	each first sub-entry is equivalent to at least one of the second sub-
16	entries; and
17	determining that the first access control is functionally equivalent to the
18	second access control list only when each of the first sub-entries is
19	equivalent to at least one of the second sub-entries;
20	wherein programmatically determining whether the first access control list is
21	equivalent to the second access control list comprises:
22	identifying a dimensional range for each policy action specified in the first
23	access control list, the dimensional range of each policy action
24	characterizing communication packets specified by entries in the first
25	access control list for that policy action;
26	identifying a dimensional range for each policy action specified in the second
27	access control list, the dimensional range of each policy action
28	characterizing communication packets specified by entries in the
29	second access control list for that policy action; and
30	determining whether the dimensional range identified for each policy action in
31	the first access control list is equivalent to the dimensional range
32	identified for each policy action in the second access control list;

33	wherein identifying the dimensional range for each policy action specified in the first
34	access control list and in the second access control list comprises at least one
35	step from a set of steps comprising:
36	identifying a source Internet Protocol (IP) address range and a destination IP
37	address range for communication packets specified by each of the
38	entries in the first access control list and in the second access control
39	list;
40	identifying a source port range and a destination port range for
41	communication packets specified by each of the entries in the first
42	access control list and in the second access control list; and
43	identifying a communication protocol for communication packets specified by
44	each of the entries in the first access control list and in the second
45	access control list.

1	27.	(Currently Amended) The policy server of claim 26, ~~wherein~~ further comprising a
2		memory to store a plurality of access control lists, including the first access control
3		list and the second access control list, and wherein the processor is configured to
4		configure each security device on the network with at least one of the plurality of
5		access control lists.

1	28.	(Canceled)

1	29.	(New) A computer system as recited in Claim 25, wherein the first access control list
2		and the second access control list each specify a plurality of entries, and each entry
3		identifies a dimensional range for a policy action, the dimensional range
4		characterizing communication packets that are to be affected by the policy action, and
5		wherein the means for programmatically determining whether a first access control
6		list is equivalent to the second access control list comprise:
7		means for determining whether each entry in the first access control list has a
8		dimensional range that is either equivalent to or contained by the dimensional
9		range of entries in the second access control list that specify the policy action
10		of the entry in the first access control list.

1 30. (New) A computer system as recited in Claim 25, wherein the first access control list
2 and the second access control list each specify a plurality of entries, and each entry
3 identifies a dimensional range for a policy action, the dimensional range
4 characterizing communication packets that are to be affected by the policy action, and
5 wherein the means for programmatically determining whether a first access control
6 list is equivalent to the second access control list comprise:
7 means for determining whether each entry in the first access control list has a
8 dimensional range that is either equivalent to or contained by the dimensional
9 range of entries in the second access control list that specify the policy action
10 of the entry in the first access control list; and
11 means for determining whether each entry in the second access control list has a
12 dimensional range that is either equivalent to or contained by the dimensional
13 range of entries in the first access control list that specify the same policy
14 action.

1 31. (New) A policy server as recited in Claim 26, wherein the first access control list and
2 the second access control list each specify a plurality of entries, and each entry
3 identifies a dimensional range for a policy action, the dimensional range
4 characterizing communication packets that are to be affected by the policy action, and
5 wherein programmatically determining whether a first access control list is equivalent
6 to the second access control list comprises:
7 determining whether each entry in the first access control list has a dimensional range
8 that is either equivalent to or contained by the dimensional range of entries in
9 the second access control list that specify the policy action of the entry in the
10 first access control list.

1 32. (New) A policy server as recited in Claim 26, wherein the first access control list and
2 the second access control list each specify a plurality of entries, and each entry
3 identifies a dimensional range for a policy action, the dimensional range
4 characterizing communication packets that are to be affected by the policy action, and
5 wherein programmatically determining whether a first access control list is equivalent
6 to the second access control list comprises:

7　　determining whether each entry in the first access control list has a dimensional range

8　　　　　that is either equivalent to or contained by the dimensional range of entries in

9　　　　　the second access control list that specify the policy action of the entry in the

10　　　　first access control list; and

11　　determining whether each entry in the second access control list has a dimensional

12　　　　range that is either equivalent to or contained by the dimensional range of

13　　　　entries in the first access control list that specify the same policy action.